

Return

Case No.:

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

Executing officer's signature

Printed name and title

Jun 10, 2024

s/ E Borden

Deputy Clerk, U.S. District Court
Eastern District of Wisconsin

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

2601 North Holton Street, Milwaukee, WI
53212, as further described in Attachment A

Case No. 24 MJ 118

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A.

located in the Eastern District of Wisconsin, there is now concealed (identify the person or describe the property to be seized):

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

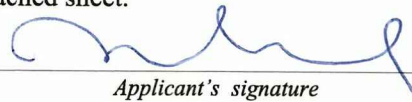
- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
21 U.S.C. 841(a)(1); 856; & 18 U.S.C. 922(g)(1)	Distribution of and possession with intent to distribute controlled substances; Maintaining a drug-involved premises; and Felon in possession of a firearm.

The application is based on these facts:
See Attached Affidavit.

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

Jacob Cowan, FBI SA

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
telephone (specify reliable electronic means).

Date: 06/10/2024



Judge's signature

City and state: Milwaukee, Wisconsin

Honorable William E. Duffin, U.S. Magistrate Judge

Printed name and title

ATTACHMENT A

Property to be searched

2601 North Holton Street, Milwaukee, Wisconsin, to include all associated common spaces, basement, attic, garage, outbuildings, sheds, and storage lockers. This address is further described as a one-story residence building, with a white in color outside entry door, with tan and red/brown colored brick, and the numbers “2601” on the silver mailbox.



ATTACHMENT B

Property to be seized

All evidence, fruits, and instrumentalities of violations of Title 21, United States Code, Section 841(a)(1) (distribution of and possession with intent to distribute controlled substances), Title 21, United States Code, Section 856 (Maintaining a Drug-Involved Premises), and Title 18, United States, Code, Section 922(g)(1) (felon in possession of a firearm), those violations involving Arthur WARD, including:

1. Controlled substances, controlled substance analogues, or listed chemicals;
2. Paraphernalia associated with the manufacture and distribution of controlled substances including but not limited to materials and items used for packaging, processing, diluting, weighing, and distributing controlled substances, such as scales, funnels, sifters, grinders, glass panes and mirrors, razor blades, plastic bags, and heat-sealing devices;
3. Duffel, canvas bags, suitcases, safes, or other containers to hold or transport controlled substances and drug trafficking related items and proceeds;
4. Proceeds of drug trafficking activities, such as United States currency, precious metals, financial instruments, and jewelry, and documents and deeds reflecting the purchase or lease of real estate, vehicles, precious metals, jewelry or other items obtained with the proceeds from drug trafficking activities;
5. Firearms, ammunition, magazines, gun boxes, firearm purchase records or receipts, and other paraphernalia associated with firearms;
6. Bank account records, loan documents, wire transfer records, money order receipts, postal express mail envelopes, bank statements, safe deposit box keys and records, money containers, financial records and notes showing payment, receipt, concealment, transfer, or movement of money generated from the sale of controlled substances, or financial transactions related to the trafficking of controlled substances;

7. Drug or money ledgers, drug distribution or customer lists, drug supplier lists, correspondence, notations, logs, receipts, journals, books, records, and other documents noting the price, quantity, and/or times when controlled substances were obtained, transferred, sold, distributed, and/or concealed;

8. Personal telephone books, address books, telephone bills, photographs, letters, cables, telegrams, facsimiles, personal notes, receipts, documents and other items or lists reflecting names, addresses, purchases, telephone numbers, addresses and communications regarding illegal activities among and between members and associates involved in drug trafficking activities;

9. Records of off-site storage locations, including but not limited to safe deposit box keys and records, and records and receipts and rental agreements for storage facilities;

10. Cellular telephones, Smartphones, text messaging systems, and other communication devices, and all electronic storage areas on the device including stored telephone numbers, recently called numbers list, text messages, digital audio and/or video recordings, pictures, settings, and any other user defined settings and/or data, as well as any records associated with such communications services used to commit drug trafficking offenses;

11. Records, items and documents reflecting travel for the purpose of participating in drug trafficking activities, such as passports, airline tickets, bus tickets, vehicle rental receipts, credit card receipts, taxi cab receipts, hotel and restaurant receipts, canceled checks, maps, and records of long distance calls reflecting travel;

12. Indicia of occupancy, residency or ownership of the premises and things described in the warrant, including utility bills, telephone bills, loan payment receipts, rent receipts, trust deeds, lease or rental agreements, addressed envelopes, escrow documents and keys;

13. Photographs, videotapes or other depictions of assets, firearms, coconspirators, or controlled substances; and

14. Computers, cellular telephones, or storage media used as a means to commit the violations described above.

15. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

c. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

f. evidence of the times the COMPUTER was used;

g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

i. records of or information about Internet Protocol addresses used by the COMPUTER;

j. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

k. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

This warrant authorizes law enforcement personnel to: (1) press or swipe the fingers (including thumbs) of WARD to the fingerprint scanner of a device found at the premises; and/or (2) hold a device found at the premises in front of WARD’s face to activate the facial and/or iris recognition features, for the purpose of attempting to unlock the device to search the contents as authorized by this warrant.

**AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A
WARRANT TO SEARCH AND SEIZE**

I, Jacob Cowan, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant pursuant to Rule 41 of the Federal Rules of Criminal Procedure to search the premises located at **2601 North Holton Street, Milwaukee, Wisconsin**, the **Subject Premises**, more fully described in Attachment A, for the things described in Attachment B.

2. I am a sworn federal law enforcement officer with the Federal Bureau of Investigation (FBI), with authority to investigate federal offenses pursuant to Titles 18, and 21 of the United States Code. I have been employed as a Special Agent with the FBI since June 2016. Prior to this, I served as an Officer in the United States Army for twelve years. I have obtained a Bachelor of Science Degree in Criminal Justice from the University of Wisconsin-Milwaukee, a Master's in Professional Studies (M.P.S.) from St. John's University, and a Post Graduate Certificate from the Kennedy School of Government at Harvard University. I graduated from the FBI Academy in Quantico, Virginia in 2016 and have over eight years of law enforcement experience. I have been involved in the enforcement and investigation of numerous violations of federal law to include drug trafficking investigations, firearm trafficking investigations, and violent crime related cases. I have personally conducted and participated in numerous investigations that have given me familiarity with the various methods that criminals use to conduct illicit firearm and narcotics transactions in violation of federal law. I have used

investigative techniques including, but not limited to: consensual monitoring, physical surveillance, witness and subject interviews, court authorized electronic surveillance, review and analysis of telephone records, and the execution of search and arrest warrants.

3. Based on my training, experience, and participation in drug trafficking and firearms investigations, I know that drug traffickers frequently possess firearms and ammunition to protect their illegal product, and that drug traffickers engaged in mobile drug trafficking often use their vehicles to facilitate their trafficking activities by transporting and/or securing contraband including but not limited to controlled substances, packaging materials and other tools of the drug trade, drug proceeds, and firearms.

4. Based upon my training and experience, I know that computer hardware and software may be important to a criminal investigation in two distinct and important respects: (1) the objects themselves may be instrumentalities, fruits, or evidence of crime, and/or (2) the objects may have been used to collect and store information about crimes (in the form of electronic data). Rule 41 of the Federal Rules of Criminal Procedure permits the government to search and seize computer hardware and software that are (1) instrumentalities, fruits, or evidence of crime, or (2) storage devices for information about crime.

5. To this end, based upon my training and experience, I know that individuals involved in drug trafficking, illegal possession of firearms, and firearms trafficking frequently use cellular telephones to maintain contact and arrange

transactions with their sources, customers, and co-conspirators. I have also found it very common for crime suspects to use their cellular telephones to communicate aurally or via electronic message in “text” format with individuals whom they purchase, trade, or otherwise negotiate to obtain illegal drugs and firearms. I also believe that it is common for crime suspects who possess illegal controlled substances and firearms to often take or cause to be taken photographs and other visual depictions of themselves, their associates, and the illegal controlled substances and firearms that they control, possess, buy, and sell.

6. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

7. Throughout this affidavit, reference will be made to case agents. Case agents are those federal, state, and local law enforcement officers who have directly participated in this investigation, and with whom your affiant has had regular contact regarding this investigation.

8. The Court has jurisdiction to issue the proposed warrant because it is a “court of competent jurisdiction” as defined in 18 U.S.C. § 2711. Specifically, the Court is a district court of the United States that has jurisdiction over the offenses being investigated; see 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

9. The Federal Bureau of Investigation ("FBI") is investigating allegations that members of the Gangster Disciples street gang, including ARTHUR WARD, are conspiring with each other, and other individuals yet unknown, to traffic firearms and transport and distribute controlled substances, namely cocaine, in Milwaukee, Wisconsin. The investigation has revealed that WARD is believed to reside in Milwaukee, Wisconsin, and that he is believed to use the **Subject Premises** to facilitate his firearm and drug trafficking activities.

10. On May 28, 2024, a confidential source (CS-2) notified law enforcement he/she was in contact with WARD about the purchase of firearms. CS-2 advised law enforcement that WARD would not text with CS-2 because WARD was being very careful due to WARD knowing he had an active warrant for his arrest. Therefore, conversations setting up the purchase of firearms from WARD by CS-2 were unrecorded calls. Law enforcement instructed CS-2 to continue to communicate with WARD in the attempt to locate him and to purchase firearms.

11. On May 28, 2024, at approximately 5:02 p.m., CS-2 contacted law enforcement and stated WARD wanted to sell CS-2 two Taurus G2 9mm firearms, one of which had an extended magazine. Law enforcement advised CS-2 to confirm with WARD that CS-2 would purchase both of the firearms.

12. On May 31, 2024, at approximately 2:30 p.m., law enforcement met with CS-2 at a pre-determined staging area. CS-2 was searched for contraband and United States

Currency (U.S.C.) with negative results. Law enforcement searched CS-2's vehicle for contraband and U.S.C. with negative results.

13. CS-2 advised law enforcement that he/she would call WARD on the way to north Milwaukee, where CS-2 believed WARD to be staying, to receive the exact address of where CS-2 would be meeting WARD to purchase firearms.

14. At approximately 2:34 p.m., at a staging area, CS-2 was given \$14,000 U.S.C. in pre-recorded buy funds. CS-2 was equipped with audio and visual recording equipment and the devices were activated.

15. Thereafter, CS-2 departed the staging area for north Milwaukee. CS-2 was followed by a law enforcement surveillance team. CS-2 drove to north Milwaukee.

16. At approximately 2:48 p.m., CS-2 placed a consensually recorded telephone call to WARD. CS-2 said, "What's the word my boy?" WARD said, "What's the word my boy?" CS-2 said, "Shit, where you at with it?" WARD said, "Shit, I'm going to be back at the house in like fifteen minutes." CS-2 said, "Like fifteen...you still at the same spot-on Appleton?" WARD said, "On Appleton?" CS-2 said, "Nigga the last time I moved your spot it was by a graveyard, right?" WARD said, "Uh yeah, yeah, yeah, yup, I ain't over there no more bro." CS-2 said, "Oh." WARD said, "I'm on Clarke and shit." CS-2 said, "You want me to come where?" There was a malfunction with the recording equipment, and during the malfunction, WARD told CS-2 to go to the **Subject Premises**.

17. At 3:24 p.m., CS-2 arrived at the **Subject Premises** and parked in front of the residence.

18. At approximately 3:28 p.m., CS-2 placed a consensually recorded call to WARD and said, "I'm all the way down..." WARD said, "Come to the side here." CS-2 said, "Alright bet." CS-2 drove down the street. WARD was still on the telephone with CS-2. CS-2 said, "You still there my boy?" WARD said, "Huh?" CS-2 said, "Mother fucking traffic busy as hell right here." WARD said, "Hell yeah (Unintelligible) [WARD spoke to an unidentified individual in the background], my nigga said he was lying, I didn't know you was out there in the front bro." CS-2 said, "Hell yeah, I'm like damn, I had called you though but your girl answered. I was like why does he have me going a fucking busy street." CS-2 said, "I see you." CS-2 parked CS-2's vehicle and exited.

19. At approximately 3:29 p.m., CS-2 met WARD at the **Subject Premises**. CS-2 said, "What's the word my boy, fuck with you?" WARD said, "(Unintelligible)." WARD was wearing red shorts and a red T-shirt. WARD was standing at the passenger seat of a white in color vehicle parked on Holton Street and retrieved a pistol. WARD put the pistol under his shirt in his shorts and walked to the side door of the **Subject Premises**. The pistol had an extended magazine. *See Figure 1.*



*Figure 1
(Depicting Arthur WARD entering the **Subject Premises** with firearm
with extended magazine)*

20. Case agents conducting surveillance at the **Subject Premises** confirmed that the individual CS-2 met with was Arthur WARD by comparing the individual they observed with a booking photograph of Arthur E. WARD (DOB xx/xx/1988).

21. Thereafter, the CS-2 followed WARD, and they entered the **Subject Premises**. Once in the **Subject Premises**, WARD and CS-2 were in the kitchen. There were multiple unidentified females and children present. WARD handed CS-2 the firearm. CS-2 removed the magazine from the firearm and WARD took the firearm back.

WARD pulled the slide of the firearm to the rear to show CS-2 there was no ammunition in the chamber. WARD then gave the firearm back to CS-2. CS-2 and WARD talked about choppers [Assault weapons] and the cost of choppers. Then, WARD said to CS-2, "(Unintelligible), I want you to come outside so you can see it bro." WARD and CS-2 continued to talk about choppers. WARD said, "Mother fuckers ain't be having no choppers." WARD said, "(Unintelligible) mother fucker be 1250 for an AR." CS-2 said, "What the hell they in the store for, 800?" CS-2 and WARD continued to talk about the prices of AR's. WARD handed what appeared to be cocaine in a clear plastic bag to CS-2 to look at. CS-2 handed the suspected cocaine back to WARD and WARD placed the suspected cocaine in his pocket.

22. During the time CS-2 was inside the **Subject Premises**, WARD was looking for his cellular telephone. Additionally, an unidentified female entered the **Subject Premises**, and WARD conducted a narcotics transaction with of what appeared to be pills with this unidentified female. Also during the time that CS-2 was inside the **Subject Premises**, WARD placed a telephone call to an unknown individual and said, "When you pull up, I'm going to come outside." Later on, WARD received a telephone call from an unidentified individual and said, "Your boy outside right now, okay, I'm coming outside right now." WARD and CS-2 walked outside.

23. Based on their training, experience, and familiarity with this investigation, case agents believe WARD had one firearm on his person that he sold to CS-2 and was awaiting the arrival of a second firearm to sell to CS-2. Case agents further believe WARD

was talking to CS-2 about the potential sale of assault weapons in the future. Case agents believe WARD showed CS-2 cocaine to entice CS-2 into purchasing cocaine from him.

24. When WARD and CS-2 went outside, they met an unidentified white female who was standing outside, who said, "I don't know if this is him in the silver car, (Unintelligible) meet in the alley." The unidentified female then said, "There he is." WARD walked over to a dark in color SUV, and the unidentified white female and WARD stayed by the **Subject Premises**. WARD stayed over by the dark in color SUV for a few minutes. WARD walked back from the dark in color SUV, and WARD and CS-2 subsequently walked back inside the **Subject Premises**. WARD handed another firearm to CS-2. In the consensual audio video recording, CS-2 was overheard pulling the slide of a firearm to rear multiple times. CS-2 and WARD agreed to talk at a later date, and CS-2 exited the **Subject Premises** and entered CS-2's covert vehicle.

25. Based on their training, experience, and familiarity with this investigation, case agents believe the unidentified white female called WARD and informed WARD that an unidentified individual arrived at the **Subject Premises** with the second firearm WARD was to sell CS-2. Case agents further believe WARD and CS-2 walked outside the **Subject Premises** where WARD met with an unidentified individual and received a firearm. Case agents believe WARD and CS-2 then walked back into the **Subject Premises** where WARD sold the second firearm to CS-2.

26. At approximately 3:53 p.m., law enforcement followed CS-2 back to the staging area.

27. At approximately 4:10 p.m., CS-2 arrived at the staging area, turned over two firearms to law enforcement: a Taurus Armas G2C 9mm pistol, bearing serial number ABC342083, and a Taurus Armas G2C 9mm pistol with and extended magazine, bearing serial number ACG990064. Both firearms were manufactured outside of the state of Wisconsin. The audio and visual recording equipment was deactivated. Law enforcement searched CS-2 for U.S.C. and contraband with negative results. Law enforcement searched CS-2's vehicle for U.S.C. and contraband with negative results.

28. CS-2 began providing information to law enforcement in September 2023. CS-2 is cooperating in exchange for consideration on pending federal drug and firearm-related offenses. The information provided by CS-2 to law enforcement agents is substantially against CS-2's penal interest. Additionally, to the extent possible, information provided by CS-2 has been corroborated by agents through external sources, including physical evidence, consensually recorded telephone calls, phone toll information, audio recordings, surveillance, controlled buys, and law enforcement databases. CS-2 has a criminal history that includes possession of a controlled substance, manufacturing and delivery of a controlled substance, armed robbery, escape, battery, domestic violence, and various motor vehicle violations and misdemeanor convictions. Within the context of the information detailed and relied upon for purposes of this affidavit, case agents believe CS-2 is credible and CS-2's information is reliable.

29. WARD has a criminal history that includes a felony conviction for possession with intent to distribute cocaine (2007). WARD has an active warrant for his

arrest for possession of a firearm-convicted of a felony, and for possession with intent to distribute cocaine.

30. On June 4, 2024, CS-2 contacted law enforcement and stated he/she had a conversation with WARD pertaining to the future purchase of additional firearms. CS-2 stated WARD had an AK-47, a Dreco, and a revolver to sell. Law enforcement inquired about WARD being able to sell a switch for a firearm, and WARD was not able to produce one. WARD and CS-2 had an additional conversation about WARD selling CS-2 cocaine. CS-2 told law enforcement WARD had multiple ounces of cocaine for sale. CS-2 said WARD was asking \$1,350 for the AK-47 and \$950 per ounce of cocaine. WARD sent a photograph via text message of the AK-47 to CS-2. Law enforcement instructed CS-2 to set up the purchase of cocaine and the AK-47. CS-2 advised law enforcement that any future controlled purchases would occur at the **Subject Premises**.

Subject Premises

31. According to law enforcement database information, as of March 2024, Johnny Thompson is listed as the apartment renter.

32. However, physical surveillance conducted by law enforcement has observed WARD enter and exit the **Subject Premises** on May 31, 2024, and as recently as the first week of June, 2024.

TECHNICAL TERMS

33. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. IP Address: The Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.
- b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
- c. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

70. As described above and in Attachment B, this application seeks permission to search for records that might be found on the **Subject Premises**, in whatever form they are found. One form in which the records might be found is data stored on a computer’s hard drive, cellular telephone, or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

71. *Probable cause.* I submit that if a computer, cellular telephone, or storage medium is found on the **Subject Premises**, there is probable cause to believe those

records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete

this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

72. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the **Subject Premises** because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media

may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely

reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to operate a website that is used for illegal conduct, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

73. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

74. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

BIOMETRIC UNLOCK

75. The warrant I am applying for would permit law enforcement to obtain from WARD the display of physical biometric characteristics (such as fingerprint, thumbprint, facial, or iris characteristics) to unlock devices subject to search and seizure pursuant to this warrant. I seek this authority based on the following:

76. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners and facial recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to use.

77. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

78. If a device is equipped with a facial recognition feature, a user may enable the ability to unlock the device through his or her face. For example, Apple offers a facial recognition feature called "Face ID." During the Face ID registration process, the user holds the device in front of his or her face. The device's camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Face ID.

79. If a device is equipped with an iris recognition feature, a user may enable the ability to unlock the device through his or her irises. For example, Samsung offers an Iris Scanner, which uses the biometric information of an individuals' irises to identify the user.

80. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

81. As discussed in this affidavit, based on my training and experience I believe that one or more digital devices will be found during the search. The passcode or

password that would unlock the device(s) subject to search under this warrant is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

82. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when (1) more than 48 hours has elapsed since the device was last unlocked or (2) when the device has not been unlocked using a fingerprint for 4 hours and the passcode or password has not been entered within a certain period of time. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

83. Due to the foregoing, if law enforcement personnel encounter a device that is subject to search and seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to (1) press or swipe the fingers (including thumbs) of WARD to the fingerprint scanner of the device; (2) hold the device in front of WARD's face to

activate the facial recognition feature; and/or (3) hold the device in front of WARD's face to activate the iris recognition feature, for the purpose of attempting to unlock the device in order to search its contents as authorized by this warrant.

CONCLUSION

84. Based upon the facts contained within this affidavit I believe there is probable cause for a warrant to search the **Subject Premises** described in Attachment A, and seize the items described in Attachment B.

ATTACHMENT A

Property to be searched

2601 North Holton Street, Milwaukee, Wisconsin, to include all associated common spaces, basement, attic, garage, outbuildings, sheds, and storage lockers. This address is further described as a one-story residence building, with a white in color outside entry door, with tan and red/brown colored brick, and the numbers “2601” on the silver mailbox.



ATTACHMENT B

Property to be seized

All evidence, fruits, and instrumentalities of violations of Title 21, United States Code, Section 841(a)(1) (distribution of and possession with intent to distribute controlled substances), Title 21, United States Code, Section 856 (Maintaining a Drug-Involved Premises), and Title 18, United States, Code, Section 922(g)(1) (felon in possession of a firearm), those violations involving Arthur WARD, including:

1. Controlled substances, controlled substance analogues, or listed chemicals;
2. Paraphernalia associated with the manufacture and distribution of controlled substances including but not limited to materials and items used for packaging, processing, diluting, weighing, and distributing controlled substances, such as scales, funnels, sifters, grinders, glass panes and mirrors, razor blades, plastic bags, and heat-sealing devices;
3. Duffel, canvas bags, suitcases, safes, or other containers to hold or transport controlled substances and drug trafficking related items and proceeds;
4. Proceeds of drug trafficking activities, such as United States currency, precious metals, financial instruments, and jewelry, and documents and deeds reflecting the purchase or lease of real estate, vehicles, precious metals, jewelry or other items obtained with the proceeds from drug trafficking activities;
5. Firearms, ammunition, magazines, gun boxes, firearm purchase records or receipts, and other paraphernalia associated with firearms;
6. Bank account records, loan documents, wire transfer records, money order receipts, postal express mail envelopes, bank statements, safe deposit box keys and records, money containers, financial records and notes showing payment, receipt, concealment, transfer, or movement of money generated from the sale of controlled substances, or financial transactions related to the trafficking of controlled substances;
7. Drug or money ledgers, drug distribution or customer lists, drug supplier lists, correspondence, notations, logs, receipts, journals, books, records, and other

documents noting the price, quantity, and/or times when controlled substances were obtained, transferred, sold, distributed, and/or concealed;

8. Personal telephone books, address books, telephone bills, photographs, letters, cables, telegrams, facsimiles, personal notes, receipts, documents and other items or lists reflecting names, addresses, purchases, telephone numbers, addresses and communications regarding illegal activities among and between members and associates involved in drug trafficking activities;

9. Records of off-site storage locations, including but not limited to safe deposit box keys and records, and records and receipts and rental agreements for storage facilities;

10. Cellular telephones, Smartphones, text messaging systems, and other communication devices, and all electronic storage areas on the device including stored telephone numbers, recently called numbers list, text messages, digital audio and/or video recordings, pictures, settings, and any other user defined settings and/or data, as well as any records associated with such communications services used to commit drug trafficking offenses;

11. Records, items and documents reflecting travel for the purpose of participating in drug trafficking activities, such as passports, airline tickets, bus tickets, vehicle rental receipts, credit card receipts, taxi cab receipts, hotel and restaurant receipts, canceled checks, maps, and records of long distance calls reflecting travel;

12. Indicia of occupancy, residency or ownership of the premises and things described in the warrant, including utility bills, telephone bills, loan payment receipts, rent receipts, trust deeds, lease or rental agreements, addressed envelopes, escrow documents and keys;

13. Photographs, videotapes or other depictions of assets, firearms, coconspirators, or controlled substances; and

14. Computers, cellular telephones, or storage media used as a means to commit the violations described above.

15. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

- a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
- b. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- c. evidence indicating the computer user's state of mind as it relates to the crime under investigation;
- d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- f. evidence of the times the COMPUTER was used;
- g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- i. records of or information about Internet Protocol addresses used by the COMPUTER;
- j. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
- k. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard

disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

This warrant authorizes law enforcement personnel to: (1) press or swipe the fingers (including thumbs) of WARD to the fingerprint scanner of a device found at the premises; and/or (2) hold a device found at the premises in front of WARD’s face to activate the facial and/or iris recognition features, for the purpose of attempting to unlock the device to search the contents as authorized by this warrant.